Office of the Information and
Privacy Commissioner of Alberta

PERSONAL INFORMATION PROTECTION ACT
Breach Notification Decision

Organization providing notice under section 34.1 of PIPA	Vari Tech Systems Inc. (Organization)
Decision number (file number)	P2018-ND-022 (File #005686)
Date notice received by OIPC	May 23, 2017
Date Organization last provided information	January 26, 2018
Date of decision	January 30, 2018
Summary of decision	There is a real risk of significant harm to the individuals affected by this incident. The Organization is required to notify those individuals pursuant to section 37.1 of the *Personal Information Protection Act* (PIPA).
JURISDICTION	
Section 1(1)(i) of PIPA "organization"	The Organization conducts business in Alberta and is an "organization" as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved all or some of the following information: • child's name, date of birth, photo, personal health number, allergies and medical information, • name of child's primary care giver and workplace, • physician name, telephone number and address, and • contact names, relationship, address, telephone number, email address, where child lives, pick up authority, emergency contact, restraining orders. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. I have jurisdiction to the extent that the information was collected in Alberta.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• The Organization provides services and web-based software for childcare centres, organizations and agencies across Canada.

	• On May 4, 2017, the Organization received a telephone call from a childcare centre in Manitoba indicating that a third party, while searching on the internet for a telephone number, was able to gain access to a report (a PDF file) containing the personal information of a child from that centre. • The Organization investigated and found the breach was caused by an unsecured folder residing on the Organization's servers. The URLs of those reports were exposed by MS Internet Explorer on Microsoft Windows 10. • When a client retrieved its report using the MS Internet Explorer browser on Windows 10, the browser registered all those URLs and sent them to Bing. Later, a Bing crawler indexed only those reports and not all reports residing on the server. • All information was recovered and is no longer available on the internet as of May 9, 2017. • The incident occurred between February 25, 2017 and May 10, 2017.
Affected individuals	The incident may have affected approximately 1,500 individuals (and their families) across Canada, including Alberta. The Organization does not know how many Albertans were affected but confirmed that one individual in Manitoba has been directly affected by the incident.
Steps taken to reduce risk of harm to individuals	• Realized that the breach was a result of clients using Microsoft Windows 10 and Internet Explorer. The computers did not have proper installation and security protection. • Immediately moved the PDF files to a separate folder at the data centre. • Added more security in production. • All users must enter a username and password to access the PDF folders. • Notified Bing/Edge/Microsoft of the breach and a formal request was made to remove all affected URL addresses and their descriptions from all search engines on the Internet. • Reviewed the site and all information was removed. • Checked the logs and confirmed no new retrievals were done since the implementation of the security measures on May 4, 2017.
Steps taken to notify individuals of the incident	The affected individual in Manitoba was notified on May 31, 2017. All other clients and centres were notified on June 16, 2017.

REAL RISK OF SIGNIFICANT HARM ANALYSIS	
Harm Some damage or detriment or injury that could be caused to affected individuals as a result of the incident. The harm must also be "significant." It must be important, meaningful, and with non-trivial consequences or effects.	The Organization reported the possible harm is minimal and that "although the information was available on the web, a person wanting to access this information would need to type very specific information into the search engine…There is a minimal possibility of identity theft as all the information was displayed all from one document opened by the childcare centre." As well, the Organization reported that "(b)ecause of the information displayed the results could have been used for identity theft, however, we do not believe this is the case…Vulnerable youth – child records were displayed." In my view, the contact information and identity information at issue could be used to cause the harms of identity theft and fraud. The medical information at issue could be used to cause the harms of hurt, humiliation and embarassment. The email address could be used for phishing purposes. These are significant harms.
Real Risk The likelihood that the significant harm will result must be more than mere speculation or conjecture. There must be a cause and effect relationship between the incident and the possible harm.	The Organization reported that it "believes only 1 stranger obtained this information because they were looking for very specific data and came across the document." The Organization said "there was only 1 report of this incident and while assessing damage, the incident was well contained" between those affected and the Organization. In my view, although the incident was as a result of human error and not malicious intent, the likelihood of harm resulting in this case is increased because an unknown third party discovered the personal information on the internet. The unknown third party notified the centre of the incident; however, the Organization does not know how many other young people and families may have been affected by this incident. Further, the information may have been exposed for approximately three months.

DECISION UNDER SECTION 37.1(1) OF PIPA

Based on the information provided by the Organization and given the circumstances of the incident, I have decided that there is a real risk of significant harm to the affected individuals.

The contact information and identity information at issue could be used to cause the harms of identity theft and fraud. The medical information at issue could be used to cause the harms of hurt, humiliation and embarassment. The email address could be used for phishing purposes. These are significant harms. Although the incident was as a result of human error and not malicious intent, the likelihood of harm resulting from this incident is increased because an unknown third party discovered the personal information on the internet. The unknown third party notified the centre of the incident; however, the Organization does not know how many other young people and families may have been affected by this incident. Further, the information may have been exposed for approximately three months.

I require the Organization to notify the affected individuals in Alberta in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

I understand the Organization notified all clients and centres on June 16, 2017. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner